103 – Image Analysis

Team Information

Team Name: @ls0-ran

Results Email: [redacted]

Examination Time Frame: to

Instructions

Description: Examine the images in the **103_Image_Analysis_Challenge2008** folder. Provide evidence as to the metadata contained or recovered for each of the files. Note not only the metadata, but why it may be of investigative interest.

Points will be awarded for the recovered metadata, the notation of metadata of possible investigative interest, and reasoning for your decision.

Total Weighted Points: 5 Total Points available per file – Total 100 Points Available

1. **Answers** – Supply the found/recovered metadata.
2. **Investigative Interest** – Supply the information that you feel is of investigative interest and why you consider it as such.
3. **Methodology** – Provide details to support your decision.

Internal Reviewer Use Only

Reviewer: Points Awarded:

Date: Review Period: to

Completed: ☐ Yes ☐ No ☐ Partial

Question 103: Image Analysis

The following command was run in cygwin on a Windows XP laptop from the 103_Image_Analysis_Challenge2008 folder:

$>../../hachoir-snapshot-2007-09-09/hachoir-metadata --level=9 * > ../Results/103/raw_output.txt

Hachoir is freely available software (www.hachoir.org) that is able to parse header data from files. The above command uses the level flag set to 9 (the highest setting) to get the maximum amount of detail. It is run against all files in the current directory (*), and the output is redirected to a file. The metadata for each file is as follows:

../../103_Image_Analysis_Challenge2008/beach_foot.jpg:

Image width: 3072

Image height: 2304

Image orientation: Horizontal (normal)

Bits/pixel: 24

Pixel format: YCbCr

Compression rate: 21.9x

Creation date: 2008-03-31 15:06:20

Camera aperture: 4.59

Camera focal: 4.9

Camera exposure: 1/400

Camera model: Canon PowerShot SD550

Camera manufacturer: Canon

Compression: JPEG (Baseline)

Producer: Adobe Photoshop CS3 Windows

Comment: JPEG quality: 94% (approximate)

Format version: JFIF 1.02

MIME type: image/jpeg

Endian: Big endian

../../103_Image_Analysis_Challenge2008/bearded_guy.jpg:

Image width: 800

Image height: 800

Bits/pixel: 24

Pixel format: YCbCr

Compression rate: 11.1x

Compression: JPEG (Baseline)

Comment: JPEG quality: 93% (approximate)

Format version: JFIF 1.02

MIME type: image/jpeg

Endian: Big endian

../../103_Image_Analysis_Challenge2008/blue_eyes.jpg.jpg:

Image width: 3072

Image height: 2304

Image orientation: Horizontal (normal)

Bits/pixel: 24

Pixel format: YCbCr

Compression rate: 46.9x

Creation date: 2008-03-24 14:43:45

Compression: JPEG (Baseline)

Producer: Adobe Photoshop CS3 Windows

Comment: JPEG quality: 94% (approximate)

Format version: JFIF 1.02

MIME type: image/jpeg

Endian: Big endian

../../103_Image_Analysis_Challenge2008/board.jpg:

Image width: 2048

Image height: 1536

Image orientation: Horizontal (normal)

Bits/pixel: 24

Pixel format: YCbCr

Compression rate: 5.9x

Creation date: 2003-05-01 10:14:13

Camera aperture: 2.8

Camera focal: 3.5

Camera exposure: 1/25

Camera model: EX-Z3

Camera manufacturer: CASIO COMPUTER CO.,LTD

Compression: JPEG (Baseline)

Producer: 1.00

Comment: JPEG quality: 94% (approximate)

MIME type: image/jpeg

Endian: Big endian

../../103_Image_Analysis_Challenge2008/bride.jpg:

Image width: 256

Image height: 354

Image orientation: Horizontal (normal)

Bits/pixel: 24

Pixel format: YCbCr

Compression rate: 5.7x

Creation date: 2008-03-31 15:50:45

Compression: JPEG (Baseline)

Producer: Adobe Photoshop CS3 Windows

Comment: JPEG quality: 99% (approximate)

Format version: JFIF 1.02

MIME type: image/jpeg

Endian: Big endian

../../103_Image_Analysis_Challenge2008/brunette.jpg:

Image width: 3072

Image height: 2304

Image orientation: Horizontal (normal)

Bits/pixel: 24

Pixel format: YCbCr

Compression rate: 5.7x

Creation date: 2005-11-23 16:34:33

Camera aperture: 4.06

Camera focal: 4.1

Camera exposure: 1/2.5

Camera model: Canon PowerShot A620

Camera manufacturer: Canon

Compression: JPEG (Baseline)

Comment: JPEG quality: 96% (approximate)

MIME type: image/jpeg

Endian: Big endian

../../103_Image_Analysis_Challenge2008/curtain_lady.jpg:

Image width: 2183

Image height: 1836

Image orientation: Horizontal (normal)

Bits/pixel: 24

Pixel format: YCbCr

Compression rate: 16.9x

Creation date: 2008-03-31 15:31:20

Compression: JPEG (Baseline)

Producer: Adobe Photoshop CS3 Windows

Comment: JPEG quality: 94% (approximate)

Format version: JFIF 1.02

MIME type: image/jpeg

Endian: Big endian

../../103_Image_Analysis_Challenge2008/eagle.jpg:

Image width: 3456

Image height: 2304

Image orientation: Horizontal (normal)

Bits/pixel: 24

Pixel format: YCbCr

Compression rate: 41.1x

Creation date: 2005-03-16 14:50:11

Camera focal: 10

Camera exposure: 1/1000

Camera model: Canon EOS 350D DIGITAL

Camera manufacturer: Canon

Compression: JPEG (Baseline)

Comment: JPEG quality: 75%

Format version: JFIF 1.01

MIME type: image/jpeg

Endian: Big endian

../../103_Image_Analysis_Challenge2008/elder_lady.jpg:

Image width: 610

Image height: 865

Bits/pixel: 24

Pixel format: YCbCr

Compression rate: 7.7x

Compression: JPEG (Baseline)

Comment: JPEG quality: 95%

Format version: JFIF 1.01

MIME type: image/jpeg

Endian: Big endian

../../103_Image_Analysis_Challenge2008/girl.jpg.jpg:

Image width: 2304

Image height: 3072

Image orientation: Horizontal (normal)

Bits/pixel: 24

Pixel format: YCbCr

Compression rate: 45.5x

Creation date: 2008-03-26 15:40:54

Compression: JPEG (Baseline)

Producer: Adobe Photoshop CS3 Windows

Comment: JPEG quality: 94% (approximate)

Format version: JFIF 1.02

MIME type: image/jpeg

Endian: Big endian

../../103_Image_Analysis_Challenge2008/girl_with_glasses.jpg:

Image width: 463

Image height: 500

Bits/pixel: 24

Pixel format: YCbCr

Compression rate: 12.2x

Compression: JPEG (Baseline)

Comment: CREATOR: gd-jpeg v1.0 (using IJG JPEG v62), quality = 95

Comment: JPEG quality: 95%

Format version: JFIF 1.01

MIME type: image/jpeg

Endian: Big endian

../../103_Image_Analysis_Challenge2008/guy.jpg:

Image width: 377

Image height: 541

Bits/pixel: 24

Pixel format: YCbCr

Compression rate: 12.7x

Compression: JPEG (Baseline)

Comment: JPEG quality: 86% (approximate)

Format version: JFIF 1.02

MIME type: image/jpeg

Endian: Big endian

../../103_Image_Analysis_Challenge2008/keyboard.jpg:

Image width: 3648

Image height: 2736

Image orientation: Horizontal (normal)

Bits/pixel: 24

Pixel format: YCbCr

Compression rate: 40.7x

Creation date: 2006-11-15 19:55:06

Camera model: Canon PowerShot G7

Camera manufacturer: Canon

Compression: JPEG (Baseline)

Comment: JPEG quality: 75%

Format version: JFIF 1.01

MIME type: image/jpeg

Endian: Big endian

../../103_Image_Analysis_Challenge2008/lady_in_tshirt.jpg.jpeg:

Image width: 150

Image height: 188

Bits/pixel: 24

Pixel format: YCbCr

Compression rate: 8.7x

Compression: JPEG (Progressive)

Comment: JPEG quality: 94% (approximate)

Format version: JFIF 1.02

MIME type: image/jpeg

Endian: Big endian

../../103_Image_Analysis_Challenge2008/leonardo.jpg:

Image width: 3072

Image height: 2304

Bits/pixel: 24

Pixel format: YCbCr

Compression rate: 45.1x

Compression: JPEG (Baseline)

Comment: JPEG quality: 75%

Format version: JFIF 1.01

MIME type: image/jpeg

Endian: Big endian

../../103_Image_Analysis_Challenge2008/pensive.png:

Image width: 1200

Image height: 687

Bits/pixel: 24

Pixel format: RGB

Compression rate: 2.4x

Compression: deflate

MIME type: image/png

Endian: Big endian

../../103_Image_Analysis_Challenge2008/sequin_girl.jpg:

Image width: 210

Image height: 271

Bits/pixel: 24

Pixel format: YCbCr

Compression rate: 6.6x

Compression: JPEG (Baseline)

Comment: JPEG quality: 95%

Format version: JFIF 1.01

MIME type: image/jpeg

Endian: Big endian

../../103_Image_Analysis_Challenge2008/spoons.bmp:

Image width: 2160

Image height: 1440

Bits/pixel: 24

Compression rate: 1.0x

Compression: Uncompressed

Format version: Microsoft Bitmap version 3

MIME type: image/x-ms-bmp

Endian: Little endian

../../103_Image_Analysis_Challenge2008/tulips.jpg:

Image width: 2272

Image height: 1704

Image orientation: Rotated 90 counter clock-wise

Bits/pixel: 24

Pixel format: YCbCr

Compression rate: 8.6x

Creation date: 2005-03-06 14:35:43

Camera aperture: 4.91

Camera focal: 5.5

Camera exposure: 1/20

Camera model: Canon PowerShot A520

Camera manufacturer: Canon

Compression: JPEG (Baseline)

Comment: JPEG quality: 96% (approximate)

MIME type: image/jpeg

Endian: Big endian

../../103_Image_Analysis_Challenge2008/veiled_lady.jpg:

Image width: 532

Image height: 753

Image orientation: Horizontal (normal)

Bits/pixel: 24

Pixel format: YCbCr

Compression rate: 15.1x

Creation date: 2007-07-18 16:04:11

Compression: JPEG (Baseline)

Producer: Adobe Photoshop CS3 Windows

Comment: JPEG quality: 94% (approximate)

Format version: JFIF 1.02

MIME type: image/jpeg

Endian: Big endian

The unique fields discovered were obtained by parsing the output file as follows:

$>cat raw_output.txt | sed -e 's/.* - //1' | grep -v Challenge2008 | sed -e 's/: .*//1' | sort -nr | uniq -c > unique_meta_fields.txt

The raw output is put through sed first to remove the prepended file information. Grep is then used to ensure that file markers are not included in our data. The output then goes back to sed to remove the appended value. Sort and uniq combine to give us only the unique fields. The following are the unique metadata fields discovered in each of these files, and their respective investigative value:

Bits/pixel - Also known as color depth, this value represents the number of bits used to represent the color of a single pixel. In an investigation, this could be used to reconstruct the settings used to capture a photo, and even determine if a specific camera was used in the activity.

Camera aperture - Specifies the size of the opening allowing light into the camera. In an investigation, this could be used to reconstruct the settings used to capture a photo, and even determine if a specific camera was used in the activity.

Camera exposure - Also known as shutter speed, this value represents the amount of time light is allowed to pass through the lens. In an investigation, this could be used to reconstruct the settings used to capture a photo, and even determine if a specific camera was used in the activity.

Camera focal - The point in air at which light is focused by the lens. In an investigation, this could be used to determine how far the photographer was from the subject, as well as reconstructing the settings/camera used.

Camera manufacturer - The company that produced the camera. In an investigation, this could be used to determine which camera was used in the activity.

Camera model - The specific model of camera. In an investigation, this could be used to determine which camera was used in the activity.

Comment - Although free by nature, this field usually designates JPEG quality, which is a result of image compression. In an investigation this could be used to reconstruct the settings/camera used.

Compression - This field designates the type of compression used, if any. In an investigation this could be used to reconstruct the settings/camera used.

Compression rate - This field designates the level of compression used, if any. In an investigation this could be used to reconstruct the settings/camera used.

Creation date - This field designates the date and time the photo was taken. In an investigation, this could be used to determine exactly when (assuming the camera time has been set correctly, or can be calibrated to real time) a photo was taken.

Endian - This field designates whether the image is big or little endian. This is useful in an investigation if the image type must be reconstructed, and can also help determine what type of system was used to process the image.

Format version - This field designates what version of the selected format was used to save the picture. This is useful in an investigation if the image type must be reconstructed, and can also help reconstruct the settings/camera used.

Image height - The height of the image measured in pixels. In an investigation this can be used to determine if the picture has been modified (cropped), and can also help reconstruct the settings/camera used.

also-ran

Image orientation - This field designates the orientation of the camera when capturing the image (horizontal / rotated). In an investigation this can be used to reconstruct the position of the subject in the photo.

Image width - The width of the image measured in pixels. In an investigation this can be used to determine if the picture has been modified (cropped), and can also help reconstruct the settings/camera used.

MIME type - This field designates the Multipurpose Internet Mail Extension (MIME) format of the file. This is useful in an investigation if the image type must be reconstructed, and can also help reconstruct the settings/camera used.

Pixel format - This field designates the color model used to represent the pixels. This is useful in an investigation if the image type must be reconstructed, and can also help reconstruct the settings/camera used.

Producer - This field designates the software used to create, alter, or save the image. This is often present in digitally modified files, and can help an investigator determine if modifications were performed, and what type of software was used in the modifications.

Question 104:

The following command was run in cygwin on a Windows XP laptop from the 104_Signature_Analysis_Challenge2008 folder:

$ file * > ../Results/104/file_output.txt

The file command attempts to classify each argument passed, and the results are output to a file, providing the following:

245.JPG: JPEG image data, EXIF standard

249.JPG: JPEG image data, JFIF standard 1.01